Research Synopsis

Entitled

'The Knowledge based Intrusion detection and Prevention model for biometric system '

Submitted to

Symbiosis International University, Pune

FACULTY OF COMPUTER STUDIES

For the degree of Doctor Philosophy

By

Prof. Maithili Arjunwadkar

Under the Guidance of

Prof. Dr. R. V. Kulkarni

Professor, SIBER, Kolhapur

Rationale and significance:

Given the spectacular rise in incidents involving identity thefts and various security threats, it is necessary to have reliable identity management systems. The traditional authentication system has been used token based security (ID cards) and Knowledge-based security (PINs or Password) to validate the identity of individuals.

Biometric systems are being widely used to achieve reliable user authentication which is a crucial component in identity management. Biometric based authentication system that uses physiological (e.g. thumb print, retina scan, iris), behavioral (e.g. voice, keystroke, touch) that claimed to provide an alternative for traditional authentication systems like password, PIN etc.

Biometric system is divided into two processes namely enrollment and authentication (verification) process. During the enrollment process physiological & Behavioral Characteristics of the user are captured by the sensor in the form of image. The different feature extractors are used to extract data from that sample image to create biometric template. The template is stored during enrollment process to be compared to the one produced during verification process in the future. The stored template and the one produced during verification process are compared by matching algorithm that produces matching result of response (Yes/NO).

The match response is then sent to the application, on which a decision algorithm is implemented for granting or denying access to the user.

However biometric systems themselves are vulnerable to a number of attacks. Attacks may be at different points (threat points) like:

- User Threats

- User/ Capture Threats
- Capture/ Extraction Threats
- Extraction/ Comparison Threats during Verification
- Extraction/ Template Storage Threats during Enrolment
- Template Storage Threats
- Template Retrieval Threats
- Administrator/ Resource Manager Threats User/ Policy Management Threats
- Policy Management Threats
- Threats to Policy Management/ Portal
- Portal Threats
- Threats to all hardware components
- Threats to all software/ firmware components
- Threats to all connections (including network threats).

Currently, there are 4 major locations for storing the template like in a token or smart card, in a central database on a server, on a workstation, or directly on the sensing device. The problems that arise from attacks on biometric systems are on increase, and as number of biometric systems being deployed is growing, this may lead to significant financial, privacy, and security related violations.

New emerging technology like Intrusion Detection System (IDS) is the best weapon used to design robust biometric security techniques. "An ounce of prevention is worth a pound of detection". Intrusion prevention (IPS) is the process of performing intrusion detection and attempting to stop detected possible incidents.

Intrusion detection and prevention systems (IDPS) are primarily focused on:

- Identifying possible incidents
- Logging information about them
- Attempting to stop them
- Reporting them to security administrators

An Intrusion Detection System detects attacks as early in stage as possible and takes appropriate action. Without such a system, applications like Bank Transactions, e-governance, fund transfer etc. where confidentiality (secrecy), integrity and availability are important objectives can lose money, goodwill and security of the country etc.

The knowledge based intrusion detection technique is useful for biometric system. Using this technique intrusion and intrusion points can be detected and preventive control can be established to stop such type of intrusion. Alarm and reporting technique is used for owner as well as the user of the system.

Aims and objectives:

Traditionally, research on computer security has focused on helping developers of systems to prevent security vulnerabilities in the systems they known before the systems are released to customers.

Knowledge based systems are artificial intelligent tools provide intelligent decisions with justification. Knowledge is acquired and represented using various knowledge representation techniques, rules, frames and scripts. The basic advantages offered by such system are documentation of knowledge, intelligent decision support, self learning, reasoning and explanation.

The Knowledge Based Intrusion Detection & Prevention Model generally aims at detecting as well as preventing attacks against biometric system. The basic task of this

model is used to monitor such systems by detecting as well as preventing any unlawful incidents which leads the systems to insecure state. This monitoring is done by checking different logs against identified intrusions rule set which is stored in the model.

The major objectives of this research are:

- To study different vulnerabilities at different points of biometric system.

  Researchers reviewed more than 100 research papers to find different vulnerabilities at different points of biometric system, available intrusion detection and prevention techniques in different applications and knowledge based systems available for different intrusion detection and prevention techniques.

- To formulate detector and report alarm modules.

  Researchers proposed Intrusion Detection and Prevention model. This model contains a scheduler to prepare a schedule to check different logs for possible intrusions, and detectors to detect normal or abnormal activity. If activity is normal then alarming and reporting has been executed. If abnormal activity is found, the rule engine fires the rule to detect intrusion point and type of intrusion. The model also contains an expert system to detect source of intrusion and suggest best possible prevention technique and suitable controls for different intrusions. This model is also used for security audit as well as alarming and reporting mechanisms. The malicious activity database is stored for future intrusion detection. To detect source tracking backward chaining approach is used. The rules are defined and stored in the Rule engine of the system. Rules for this model is developed using JESS (Java Expert system Shell)

- To design rule set for vulnerabilities at each point of the biometric process.

  We designed three different agents, which can be deployed on biometric storage, biometric device and feature extraction module.

  1. Researchers have designed intelligent agent as knowledge based Biometric Template storage Intrusion Detection tool. This intelligent

agent can be located on the Biometric Template storage database. It performs intrusion detection using Operating System's audit trail, and RDBMS audit trail. The system consists of a user interface module, an inference engine, a knowledgebase of illegal transactions and audit trail of ORACLE database. Using backward chaining approach we detect source of intrusion. Inference engine is implemented using JESS which is a Java based Expert System.

2. Researchers have designed intelligent agent as knowledge based Biometric Device Intrusion Detection tool which is an innovative design. This intelligent agent can be located on the Biometric device. It performs intrusion detection using Operating System's audit trail and device manager information. The system consists of a user interface module, an inference engine, a knowledgebase of illegal transactions and certified biometric devices. Inference engine is implemented using JESS which is a Java Expert System Shell.
3. This agent is required to detect intrusions like Trojan Horse, Replay attack and Denial of Service (DoS). Plenty of IDS are available to detect those types of attack. Researchers compared available IDS and suggested Snort and Tripwire that can be useful.

- To detect source of intrusion using backward chaining approach of expert system.

  Researchers have designed more than 128 Fuzzy rules as well as non-fuzzy rules to find out priority to prevent those intrusions which are already detected by designed intelligent agent as knowledge based Biometric Template storage Intrusion Detection tool. Rules for this model are developed using Fuzzy JESS.

- To design different preventive controls using intelligent models or phenomenon.

  Researchers developed protection module of bio-hashing technique using Session key. This key is generated using Chaos phenomenon. Module is developed in JAVA.

Artificial Intelligence (AI) techniques which can be used for IDPS are data mining, artificial neural networks, fuzzy logic, Genetic algorithm and expert systems etc

They can be integrated with traditional procedural and statistical methods to analyze the collected data by sensors recognize reconnaissance patterns filter correlate events to support security event management and prevention of intrusions.

The overall objective of this Intrusion Detection and Prevention model research is to find efficient and robust model to improve the security of existing and future systems.

Scope of the study:

The intrusion detection is an essential supplement for traditional security system. This security system needs the

- robust automated auditing
- intelligent reporting mechanism
- robust detection and prevention techniques.

This system is divided into 3 sub systems:

- Intrusion detection
- Backtracking of intrusion source
- Prevention techniques.

The basic task of this model is used to monitor such systems; by detecting as well as preventing any unlawful incidents which leads the systems to insecure state.

The Knowledge based intelligent intrusion detection and prevention model for biometric system contains a scheduler to prepare schedule to check different logs for possible intrusions, and detectors to detect normal or abnormal activity. If abnormal activity is found then the rule engine checks the rule to detect intrusion point and type of intrusion. The model also contains an expert system to detect source of intrusion and suggests best possible prevention technique and suitable controls for different intrusions. This model

also uses security audit as well as alarming and reporting mechanisms. The malicious activity database is stored for future intrusion detection. To detect the source by tracking, backward chaining approach is used. The rules are defined and are stored in the Rule engine of the system. Different prevention techniques are to be developed for preventing those attacks.

- **Publication:**

a) **Papers Published**

1. Published research paper "Robust Security Model for Biometric Template Protection Using Chaos Phenomenon" in International Journal Of Computer Application in June 2010, Volume 3-Number 6

   ISBN: 978-93-80746-33-3
   ISSN 0975 - 8887. doi : 10.5120/737-1036

   Abstract

   Modern biometric technologies claim to provide alternative solution to traditional authentication processes. Even though there are various advantages of biometric process, it is vulnerable to attacks which can decline its security. Different schemes are proposed to protect from different attacks. This paper presents biometric process, attacks on biometric process, study of different protection techniques used to protect against different attacks. The authors have designed protection model of bio-hashing technique using Session key. This key is generated using Chaos phenomenon.

2. Published research paper "Rule Based Intrusion Detection and Prevention Model for Biometric System" in the Journal of Emerging Trends in Computing and Information Science in October 2010, Volume 1-Number 2.

   E-ISSN 2218-6301

   Abstract

   Modern biometric systems claim to provide alternative solution to traditional authentication processes. Even though there are various advantages of biometric

process, it is vulnerable to attacks which can decline its security. The intrusion detection is an essential supplement of traditional security system. This security system needs the robust automated auditing, intelligent reporting mechanism and robust prevention techniques. We suggest rule based intelligent intrusion detection and prevention model for biometric system. This model contains a scheduler to prepare a schedule to check different logs for possible intrusions, and detectors to detect normal or abnormal activity. If activity is abnormal then alarming and reporting is executed. If abnormal activity is found, the rule engine fires the rule to detect intrusion point and type of intrusion. The model also contains an expert system to detect source of intrusion and suggests best possible prevention technique and suitable controls for different intrusions. This model is also used for security audit as well as alarming and reporting mechanisms. The malicious activity database is stored for future intrusion detection. To detect source tracking backward chaining approach is used. The rules are defined and stored in the Rule engine of the system.

3. Published research paper "A Review: The knowledge Based Intrusion Detection and Prevention Model for Biometric System" in the International Journal Of Computational Intelligence and Information security, in June 2011 Volume 2 No.6.

   ISSN 1837-7823

   Abstract

   Even though there are various advantages of biometric authentication process, it is vulnerable to attacks, which can decline its security. To enhance the security of biometric process, Intrusion detection and prevention (IDPS) techniques are significantly useful. An IDPS detects insecure state and suggests prevention technique. The knowledge-based intrusion detection and prevention model uses the knowledge accumulated about specific task or state and system vulnerabilities. The intrusion-detection system contains information about these vulnerabilities and looks for attempts to exploit them. In this paper we review biometric process vulnerabilities and available intrusion detection and prevention models for information security and study different techniques available for knowledge based

intrusion detection and prevention model. Conclusions are drawn and directions for future research are suggested.

4. Published research paper "The Intelligent Intrusion Detection Tool for Biometric Template Storage" in the International Journal of Artificial Intelligence in Jan 2012 Volume 3-Number 1

   Impact factor value: ICV: 4.89

   ISSN: 2229–3965 (Print) & E-ISSN:2229–3973 (Online)

   Abstract

   While there are various advantages of biometric authentication process, it is vulnerable to attacks, which can decline its security. To enhance the security of biometric process, Intrusion detection techniques are significantly useful. In this paper, we have designed intelligent agent as knowledge based Biometric Template storage Intrusion Detection tool. This intelligent agent can be located on the Biometric Template storage database. It performs intrusion detection using Operating System's audit trail, and RDBMS audit trail. The system consists of a user interface module, an inference engine, a knowledgebase of illegal transactions and audit trail of ORACLE database. Inference engine is implemented using JESS which is a Java based Expert System.

5. Published research paper "Biometric Device Assistant Tool: Intelligent Agent for Intrusion Detection at Biometric Device using JESS" in the International Journal of Computer Science Issues, in November 2012, Volume 9 No.6.

   ISSN 1694-0814

   Abstract

   While there are various advantages of biometric authentication process, it is vulnerable to attacks, which can decline its security. To enhance the security of biometric process, Intrusion detection techniques are significantly useful. In this paper, we have designed intelligent agent as knowledge based Biometric Device Intrusion Detection tool which is an innovative design. This intelligent agent can be located on the Biometric device. It performs intrusion detection using Operating System's audit trail and device manager information. The system consists of a user interface module, an inference engine, a knowledgebase of

illegal transactions and certified biometric devices. Inference engine is implemented using JESS which is a Java Expert System Shell.

6. Submitted research paper for publication "Prioritization of detected intrusion for preventive action is developed using Nero-Fuzzy approach" in the Journal of Computing, in December 2012, Volume 4 No.12.
   ISSN: 2151-9617 (registered with the Library of Congress, USA)
   eISSN 2151-9617

   Abstract

   The biometric authentication process is vulnerable to attacks, which can decline its security. To enhance the security of biometric process, Intrusion detection and prevention techniques are significantly useful. In this paper, a Neuro-Fuzzy approach is used to decide priorities for detected intrusions in biometric template storage to implement preventive actions. A Neuro-Fuzzy approach is used. We used FuzzyJess and Java to achieve this prioritization. Priority table is produced as output which is useful to security administrator to implement preventive actions for detected intrusion in biometric Templatestorage.

b) **Citation**

1. Cited our research paper "Rule Based Intrusion Detection and Prevention Model for Biometric System" in the Journal of Emerging Trends in Computing and Information Science in October 2010, Volume 1-Number 2. in "A Novel approach of Intrusion Detection and Prevention for fingerprints" by Vuda Sreenivasrao in the International Journal Computer Science and Technology in Dec 2010 Volume 1-Number 2

c) **Financial Assistance from UGC**

1. UGC granted financial assistance of Rs. 1,35,000/- under the scheme of minor projects for my research topic entitled "Knowledge Based Intrusion Detection and Prevention Model for Biometric Process" (File No 47-1846/11(WRO))

- ***Bibliography:***

1. "Computer System Intrusion Detection: A Survey", By Anita K. Jones and Robert S. Sielken
2. "Feature deduction and ensemble design of Intrusion detection system", By Srilatha Chebrolu, Ajith Abraham,Johnson Thomas Computer & security (2004)
3. "An Intrusion detection system expert system with fact based" ,By Yuan Yuan,Dai Guanzhong Asian Journal of Information Technology 6(5) 614-617, 2007
4. "The Application of Generic Neural Network in Network Intrusion Detection" By Hua Jian, Junhu Ruan in Journal of computers vol 4 no 12 December 2009.
5. "Design & Implementation of rule based expert system for fault management", by Su Myat Soe and Paing Paing Zaw in World academy of science , engineering & technology 48 2008
6. Artificial neural network notes.
7. "A Comparative Analysis of Artificial Neural Network Technologies in Intrusion Detection Systems", by Shahbaz Pervez, Iftikhar Ahmad, Adeel Akram, Sami Ullah Swati
8. "Intelligent system for information security Management: architecture & design issues", by Marina Hentea in Informing science & information technology vol. 4 2007.
9. "Neural Network Learning based chaos", by Truong Quang Dang Khoa & Masahiro Nakagava in International Journal of computer & system Science & engineering 1:2 2007
10. "One way hash functions based on neural network", by Shiguo Lian,Jinsheng sun, Zhiquan Wang
11. "Novel Attack Detection Using Fuzzy Logic and Data Mining", by Norbik Bashah Idris and Bharanidharan Shanmugam
12. "Detecting Computer Intrusions Using Behavioral Biometrics", by Ahmed Awad E. Ahmed, and Issa Traore
13. "Password based a generalize robust security system design using neural network", By Manoj Kumar Singh In IJCSI international Journal of computer science issue vol 4 no 2,2009
14. "An Introduction to Intrusion Detection", *by* Aurobindo Sundaram
15. "On artificial Intelligence approaches for network Intrusion detection systems", by Sattar B. Sadkhan in MASUAM Journal of computing vol. 1 issue 2 , September 2009.
16. "A Backpropagation Neural Network for Computer Network Security", by Khalil Shihab

17. “An analysis of minutiae matching strength” by N.K.Ratha , J.H. Connell and R.M. Bolle Proc AVBPA 2001, Third international conference on Audio and video based biometric person authentication pp 223-228 2001.
18. “Attacks on biometric systems: A case study in fingerprints” by Ummat Uludag , Anil Jain
19. “Biometric Evaluation Methodology Supplement [BEM]“ Produced by the Common Criteria Biometric Evaluation Methodology Working Group Version 1.0 August 2002
20. “Biometric risk and controls”, by Christos K. Dimitriadis in Information Systems control Journal Vol 4 2004
21. “Fuzzy sets,” by L. A. Zadeh , Information and Control, pp. 338-353, 1965.
22. “Fuzzy Reasoning in Jess: The FuzzuJ Toolkit and FuzzyJess”, by Orchard, R. Proceedings of the ICEIS 2001, Third International Conference on Enterprise Information Systems, Setubal, Portugal. July 7-10,2001. Pp 533-542. NRC 44882.
23. “Biometrics based identifiers for digital identity management”, by Abhilasha Bhargav-Spantzel , Anna Squicciarini, Elisa Bertino, Xiangwei Kong, Weike Zhang, , published in Proceeding IDTRUST '10 Proceedings of the 9th Symposium on Identity and Trust on the Internet ©2010 table of contents ISBN: 978-1-60558-895-7 doi>10.1145/1750389.1750401
24. “A secured fingerprint authentication system”, by Md Rajibul Islam, Md Shohel sayeed and Andrews Samraj published in applied sciences 8(17): 2939-2948, 2008 ISSN 1812-5654 © 2008 Asian Network for scientific Information
25. “Biometric Template Protection : A Key mixed Template approach” ,by Shih-Wei Sun, Chun-Shien Lu and Pao-chi chang , published in 1-4244-0763-X/07 @ 2007 IEEE.
26. “Template and Database Security in Biometrics Systems: A Challenging Task” , by Manvjeet Kaur, Dr. Sanjeev Sofat and Deepak Saraswat, , published in International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010
27. “Detection of the Security Vulnerabilities in Web Applications” , by Marius POPA, published in Informatica Economică vol. 13, no. 1/2009 127
28. “Storage-based Intrusion Detection: Watching storage activity for suspicious behavior”, by Adam G. Pennington, John D. Strunk, John Linwood Griffin, appeared in Proceedings of the 12th USENIX Security Symposium Washington, DC. August 2003.
29. “Detecting a denial of service using artificial intelligent tools, genetic algorithm” Maath. K. Al-anni and V. Sundarajan, published in the Indian Journal of Science and Technology Vol.2 No 2 (Feb. 2009) ISSN: 0974-6846

30. “Evaluating Attack Resiliency for Host Intrusion Detection Systems”, by Jesus Molina and Michel Cukier, published in Journal of Information Assurance and Security 4 (2009) 001-009.

Maithili Arjunwadkar	Prof. (Dr.) R. V. Kulkarni	Brig. K. K.V. Khanzode
Signature (Student)	**Signature (Guide)**	**Signature (Dean)**

Date : 10th Jan 2013